Fairfax County Internal Audit Office

Fire and Rescue Department
Fairfax Inspections Database Online Application Audit
Final Report

June 2011

"promoting efficient & effective local government"

Created: April 2011

Attachment E

Executive Summary

In March 2006, Department of Public Works and Environmental Services (DPWES) and Department of Planning and Zoning (DPZ) replaced the county's legacy Inspection Services Information System with a commercial-off-the-shelf application, the Fairfax Inspections Database Online (FIDO) application. The FIDO application provides a single software solution that meets the needs of the multiple agencies involved in permits, inspections, licenses, fee collection, and complaints management processes. Currently DPWES, DPZ, Fire and Rescue Department (FRD), Health Department, and the Department of Code Compliance use the FIDO application.

This audit was a second phase examination of the FIDO system. Our first FIDO Audit covered DPWES and the report was issued in April 2010. This audit focused on the evaluation of the use of the FIDO application by FRD. FRD utilizes the FIDO application to process various permits application and inspections. Our audit found that permit inspection fees were calculated correctly by the FIDO application, and accounts receivable were monitored by FRD to maximize the collection of the inspection fee payments. Daily cash drawer reconciliations were performed to ensure payments were recorded correctly into the FIDO application. However, controls over account management, separation of duties, timeliness of inspection data input and data reviews could be strengthened. The primary issues noted were:

- Out of 60 inspection reports samples, we noted that 7% were not updated into FIDO on a timely manner and 70% did not have evidence of a review by inspection group supervisors after the inspection data was input into FIDO. Additionally, FRD did not have in place a formal written procedure for the inspection data entry and review.
- We noted that all users in both the cashiering group and cashier supervisor group had update access to the inspection test/time data entry, which gave them the ability to change the inspection fees. However, the cashiering group users had job functions which did not necessitate the need to have this additional access.
- Controls to determine whether all the inspection fees generated by FIDO were billed to the customer needed to be strengthened, as there was not a procedure in place for periodically reviewing a report of unpaid FIDO inspection fees.
- FRD was not using an access request form to document the user access authorization process. A draft form was developed but was not being used as of the end of fieldwork. While FRD reviewed the FRD user access list twice a year, they didn't keep sufficient documentation to support the process, nor did they develop formal written policy and procedures defining how the review was to be performed nor the frequency.

Scope and Objectives

This audit was performed as part of our fiscal year 2010 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit covered the period of April through December 2010, and our audit objectives were to determine that:

- All the forms of application information were input into the FIDO application in a complete and timely manner and updated properly.
- Fee payments were calculated correctly and collected in a timely manner.
- Access controls and separation of duties were established to ensure data was adequately protected from unauthorized amendment, loss, or leakage.

Methodology

Our audit approach included a review and analysis of internal controls over the FIDO application inspection data input, inspection fees billing and collection process. We interviewed appropriate employees to understand the different types of inspections, inspection fees' data entry, and billing and collection process. We observed employees' work functions; determined if controls were in place to prevent data from unauthorized modification, and tested inspection data entry, inspection fees, invoice generation and inspection fee payment collection on a sample basis.

Our audit did not examine all general controls, such as system software and security program planning and management over the FIDO application. Our transaction testing did rely on those controls; therefore, this was a scope limitation. The potential impact of this circumstance on our findings was that some portion of transaction data may be erroneous.

Findings, Recommendations, and Management Response

1. Inspection Data Entry

We randomly selected 60 inspection reports and reviewed the data in FIDO. We noted that four of them were not updated into FIDO on a timely basis and four of the inspection dates were not recorded correctly into FIDO. We also noted that for 42 of the sample transactions, supervisors did not document their review of the inspection data in FIDO to ensure it was updated correctly and completely.

FRD verbally instructed inspectors to update inspection results into FIDO no later than the following business day after the inspector performs the inspection. In addition, all data input should be validated to ensure transactions are recorded accurately and completely into the system.

The revenue and records group cannot generate timely and accurate inspection fee invoices without inspection results accurately input into the FIDO application. This could cause loss of revenue and poor customer relations through erroneous billing.

Recommendation: We recommend that FRD establish a formal written procedure to ensure all the inspection results are recorded in FIDO on a timely basis, and supervisors review the inspection data for accuracy after data entry. Supporting review of transactions should be documented.

Management Response: A written FIDO Business Procedure has been distributed to all branches. The procedure meets the audit recommendations to enter an inspection on a timely basis and to require documented supervisory review. This item was completed on April 29, 2011.

2. User Access Controls

We noted that all the users in both the cashiering group and the cashier supervisor group had update access to the inspection test/time data entry. Inspection fees were generated based on the inspection data that inspectors input into the system including the test/time data field. Per discussion with FRD, only the supervisor of the revenue and records group needed this access to make corrections or updates to FIDO records in a timely manner. Neither the cashiering group nor the cashier supervisor group user profiles can alter the inspection status detail records. Additionally, we noted that four users were assigned to both the cashiering group and the inspectors group in the FIDO application giving them access to update inspection status and post payments.

Fairfax County Information Technology Security Policy 70-05.01, states: “Access control shall be implemented along with procedures that stipulate and safeguard access to county information only to those with privileges necessary to perform their job function. The concept of “least privilege” should be followed.” The cashier and cashier supervisor have responsibilities for payment processing, not inspections. Giving them update access may increase the risk of an erroneous inspection status being posted.

Recommendation: We recommend that FRD implement least privilege access controls when granting user access rights to the user group profile. Users in the cashiering group should not have update access to the inspection test/time data entry. In addition, FRD should not assign users to both the cashiering group and inspector group.

Management Response: The cashiers that are employed in Revenue and Records as cashiers were removed from the FPD Inspections Group under Help Desk Service Request 620642. The FPD Cashier Group was updated to remove rights to all Inspection Test Time Entry fields under Help Desk Service Request 620654. This item was completed on April 13, 2011.

3. Unpaid Inspection Fees

We randomly selected 60 inspection reports to determine whether all the inspection fees were billed to the customer in a timely manner, and if fee payments were collected. Among the 60 samples, we noted that an invoice was not generated and fee payment was not collected for one inspection report. Upon further investigation, we discovered that the current reconciliation process would not catch unpaid fees in FIDO not recorded FAMIS.

The Department of Finance conciliation of Financial Transactions Policy (ATB 10020) states: "All discrete business units (departments) of the County, including departments, agencies, offices, courts, authorities and boards, are required to ensure the integrity of financial transactions posted to the County's financial systems by performing monthly reconciliation in accordance with Reconciliation Plans (Plan) developed by the departments and approved by the Department of Finance."

FRD did not set up an exception report and run it periodically to determine whether all the inspection fees generated by FIDO were billed to the customer. Unbilled inspection fees could potentially result in loss of collection of revenues earned from inspection services the county provided.

Recommendation: We recommend that FRD run a bi-weekly exception report for unpaid FIDO inspection fees. The revenue and records group manager should review the exception report to ensure that FRD has generated bills for all the inspection fees.

Management Response: A FIDO Unpaid Fees report has been created. The report can be generated against any chosen date range. The revenue and records supervisor or designee will run the report bi-weekly and review it for accuracy. This item was completed on April 29, 2011.

4. User Access Authorization Documentation

For the audit period tested, FRD did not have a formalized process to grant and document user access. The FRD FIDO project manager received the request for adding or changing user access rights to the FIDO application through e-mail or phone conversation. FRD did not keep all the e-mail communications for the requests of changing user access rights to the FIDO application. Fairfax County Information Technology Security Policy 70-05.01 states that, "all accounts created shall have an associated request and approval that is appropriate for the Fairfax County system or service. System administrators or other designated staff:

- Are responsible for removing the accounts of individuals who change roles within Fairfax County or are separated from their relationship with Fairfax County.
- Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes."

The lack of a standardized access request form creates risks of granting users excessive access rights, adding new users, or changing users' access rights without manager's approval, and keeping transferred or terminated users active in the system.

Recommendation: FRD developed a draft standard user access request form at the beginning of this audit; however, they had not started to use this form to document user access authorizations. We recommend that FRD finalize their standard access request form to document authorization and modification of access privileges approved by an authorized manager and maintain the completed forms on file. Additionally, formal written procedures should be developed and communicated to employees.

Note: Discussion with FRD management indicated that FRD had finalized a standard user access request form and provided it to the branch managers during the issuance process of this report.

Management Response: A written FIDO Business Procedure, User Access Authorization, and a User Access Request form have been developed. The form was distributed to all employees by e-mail on April 5, 2011. The written business procedure was distributed on April 29, 2011. This item was completed on April 29, 2011.

5. User Access Maintenance

The FRD FIDO system administrator reconciled the FIDO FRD user access list to the Fire Headquarters Position Occupancy report twice a year. FRD kept digital copies of the reconciled lists; however, the FIDO FRD user access list and the Fire Headquarters Position Occupancy Report were discarded after reconciliation. Also, FRD had not developed written procedures covering the reconcilement process.

Fairfax County Information Technology Security Policy 70-05.01 states that, "system Administrators or other designated staff shall have a documented process for periodically reviewing existing accounts for validity."

Failure to maintain source documents for the reconciliation and establish written policies defining frequency requirements decreases the accountability for performing the review. This increases the risk of non-performance, which allows users with inappropriate access to critical or sensitive resources to pose a threat, especially those individuals who may have left under acrimonious circumstances.

Recommendation: We recommend that FRD document procedures to periodically review the FIDO application user list and document the user account validation process. Additionally, FRD should keep all the supporting documentation for the user list review.

Management Response: A written FIDO Business Procedure, User Access Maintenance, has been written to ensure a consistent reconciliation process. This item was completed on May 11, 2011.